技術ガイド

IdP, SPの構築に関する講習会を行っております。詳しくは、イベントガイドをご覧ください。
※この技術ガイドは、講習会（実習セミナー）のテキストも兼ねています。

実習セミナー

- OSへのログインなど、全ての作業をrootユーザにて行っていますが、実習セミナーの時間短縮の為であり、実作業では推奨致しません。
- 実習セミナーの構築手順について
  IdP構築は★印で、SP構築は★印を付けています。目印に作業を進めてください。
  まず、構築手順前の事前準備を行います。
  →「実習セミナー環境について（シンクライアント環境は、こちら）」を参照してください。

更新情報

- Shibboleth環境構築セミナー（活用編）
  2024/05/31 • 更新者 : Takeshi Nishimura • 変更の表示
  運用責任者・運用担当者の指名・交代および情報変更の方法について
  2024/05/20 • 更新者 : Takeshi Nishimura • 変更の表示
  eduGAINに関する情報
  2024/04/22 • 更新者 : Takeshi Nishimura • 変更の表示

  ※ 技術ガイド外のページも一部含まれます

IdP

- IdPの概要
- インストール
  - 貴学にてIdPv4をインストールする場合の構築手順
- 設定・運用・カスタマイズ
- IdP構築関連ファイル
- Shibboleth環境構築セミナー（活用編）

SP

- SPの概要
- インストール
  - 貴学にてSPをインストールする場合の構築手順
- 設定・運用・カスタマイズ

- SP構築関連ファイル
- Shibboleth環境構築セミナー（活用編）

属性

学術認証フェデレーションで利用を推奨する属性のリストを提供します。

- 属性リスト

以下は、SPを構築した際に受信した属性を表示するためのサンプルスクリプトです。

- 属性確認用PHPプログラム
  このプログラムはApache上で動作することを前提としたものです。

- Apache以外での属性値取得については以下に情報があります。
  ⇒GakuNinShare:設定・運用・カスタマイズ#Apache以外の環境で属性値を取得する方法
- $checkScopedAttributeフラグにてスコープのチェック機能を持ちますが、通常は不要です。有効化する場合はコメントの指示に従ってShibboleth SPの設定を行った後、慎重に行ってください。

なお、運用フェデレーションでのIdPの送信属性確認には、学認技術運用基準の9.2に記載されております「属性表示サービス」をご利用ください。attrviewer20, attrviewer13
テストフェデレーションでの接続試験に関しては、テストフェデレーションルールに記載されております。test-sp1, test-sp2, test-sp3
⇒テストフェデレーションルール

メタデータ

学認が提供するメタデータ（フェデレーションメタデータ）は新規IdP／新規SPの追加や、既存IdP／既存SPの証明書の更新等により、常に更新されます。そのため、定期的にリポジトリから最新のメタデータをダウンロードしてIdP/SPのメタデータを更新してください。
また、使用証明書の更新等、自分の管理するIdP/SPのメタデータに変更があった場合は、学認申請システムより変更申請を行って下さい(*)。

⚠ 2017年11月17日から署名証明書の変更に伴いメタデータURLも変更になっております。詳細はメタデータ署名検証用証明書（署名証明書）を参照してください。

- 公開URL https://metadata.gakunin.nii.ac.jp/gakunin-metadata.xml
- メタデータ署名検証用証明書（署名証明書）

テストフェデレーションのメタデータについてはテストフェデレーションルールを参照してください。 ⇒テストフェデレーションルール

(*) - 自組織のIdP/SPのメタデータの更新について、特に、使用証明書の更新については途切れることなくサービスを提供するためには注意が必要です。
それぞれのページにてご確認ください。
IdPの証明書更新　／　SPの証明書更新

※ メタデータに設定されているvalidUntilについて

※ IdP/SP個々のメタデータ（エンティティメタデータ）の内容については次のテンプレートの項をご参照ください。

テンプレート

属性設定とメタデータのテンプレートを提供しています。下記をクリックして必要なテンプレートをダウンロードしてご利用ください。ご利用方法は、上記のIdP,SP構築方法をご参照ください。メタデータに関しましては、学認申請システムにて自動生成されますので、本テンプレートは補助的な目的でご利用ください。

- 属性設定テンプレート（IdP用）
  利用方法はIdP設定の attribute-resolver.xml / attribute-filter.xml をご参照ください。
  - attribute-resolver.xml（共通）
  - attribute-filter.xml（運用フェデレーション用）
  - attribute-filter.xml（テストフェデレーション用）
  - gakunin-rules.tar.gz（共通）
    - /opt/shibboleth-idp/conf/ 以下で展開する（/opt/shibboleth-idp/conf/attributes/custom/以下に*.propertiesが配置される）ものです。
    - Shibboleth IdPバージョン4(V4)およびそれ以降用の新規のファイル群です。Attribute Registryに学認で規定されている（かつ配布物に含まれない）属性を追加します。
    - 本ファイルはV4用のattribute-resolver.xmlと組み合わせて使うものです。典型的にはV4の新規インストール時に使用します。V3からのアップグレードの場合、V3もしくはそれ以前用のattribute-resolver.xmlテンプレートを使っている場合に限り本ファイルは不要ですが、将来的にV4テンプレートに更新するのに備えてV4環境にはインストールしておくことを推奨します。

> **更新情報2023年8月24日(4.2.0)**
>
> Shibboleth IdP 4.2.x 向けに attribute-resolver.xml のテンプレートを公開しました。
>
> **更新情報2021年10月22日(4.1.0)**
> Shibboleth IdP 4.1.x向けにattribute-resolver.xmlのテンプレートを公開しました。V4の新機能のSAML Proxyを使うような場合は最新版をお使いになることを推奨します。
>
> **更新情報2021年7月19日(4.0.1)**
>
> LDAP DataConnectorにて exportAttributes="" （空文字列）という形でテンプレートを公開しておりました（コメントに記述しておりますようにLDAPから直接送出したい属性を列挙するものです）が、未修正のまま実行すると以下のような意味不明なエラーに

なってしまうため、ダミーの属性名を入れております。ご利用の際はダミーを取り除いて正しい属性名で置き換えて（もしくは不要な場合は exportAttributes="..." の部分自体を削除して）ください。

```
net.shibboleth.utilities.java.support.service.ServiceException: org.springframework.beans.factory.xml.
XmlBeanDefinitionStoreException: Line NNN in XML document from file [/opt/shibboleth-idp/conf/attribute-resolver.
xml] is invalid; nested exception is org.xml.sax.SAXParseException; lineNumber: NNN; columnNumber: NN; cvc-minLength-
valid: 長さが'0'である値''は、タイプ'string'のminLength '1'に対してファセットが有効ではありません。
```

更新情報2020年8月11日(4.0.0)

以前のテンプレートからの更新で、かつプロパティ idp.pool.LDAP.failFastInitialize をtrueにして使ってる場合はテンプレートを最新版に切り替えたタイミングで起動時LDAPに接続できなかった場合の挙動が変わる可能性があります（当該プロパティを参照しなくなったため）。IdP起動時にLDAPに接続できなければエラーにする（デフォルトの挙動ではありません）場合はLDAP Connectorに failFastInitialize="true" を追加してください。

Shibboleth IdP 4で利用するためのテンプレートです。

以下の通りV4の新機能と整合性を取るため属性名の見直しを行いましたので、他の設定とマージを行う場合はご注意ください。なお、新属性名は学認技術運用基準で規定される属性の「friendlyName」に記載されているものです。旧属性名は同規程の「名称」に記載されているものでした。

3.4.0まで	4.0.0以降
organizationName	o
organizationalUnitName	ou
surname	sn
jaOrganizationName	jao
jaOrganizationalUnitName	jaou
jaSurname	jasn

また今回のLDAP Connectorから、V4の新機能であるAttribute Registryを使ってLDAP DataConnectorのexportAttributesに指定することでLDAPの値を直接送出するようになっています。単純なSimple AttributeDefinitionが削減可能です。詳細はファイル中のコメントを参照してください。

またeduPersonTargetedIDの設定について、以前のテンプレートではソース属性の存在（AttributeDefinitionを定義しているかどうか）によってコメントアウトを解除するかどうかで切り替えていたものが、今回の版からソース属性のタイプによってInputAttributeDefinitionにするかInputDataConnectorにするかを切り替える形に変更になっています。詳細は該当部分のコメントを参照してください。

今回からeduPersonTargetedID(ComputedId,StoredId)のエンコード方法がプロパティ idp.persistentId.encoding の値を反映するようになっています。以前のバージョンから引き続き本バージョンおよびそれ以降をお使いになる場合は、現在使っているエンコード方法を調査し、saml-nameid.properties に記載の値と差異がある場合は当該ファイルを修正の上本バージョンを適用してください。

調査の例:
使用している attribute-resolver.xml のComputedId/StoredId DataConnectorに
- encodingが設定されていなければBASE64、
- 固定値（BASE64もしくはBASE32）が設定されていればその値、
- すでに上記プロパティを参照しているなら修正の必要なし。

Shibboleth IdP 3.4.x向けテンプレート - 3.4の配布物をベースとして再作成しました。

Shibboleth IdP 4.0で廃止予定の設定を代替の方法に修正、もしくは削除しました。
詳細: https://wiki.shibboleth.net/confluence/display/IDP30/DeprecatedIdPV4

ダウンロード: attribute-resolver-template-3.4.0.xml, attribute-filter-template-prodfed-3.4.0.xml, attribute-filter-template-testfed-3.4.0.xml
Shibboleth IdP 3.3.x向けテンプレート - attribute-resolver.xmlにおいても名前空間を省いたフラット化を行いました。

学認技術運用基準(v2.2)に新たに追加された属性 eduPersonAssurance, eduPersonUniqueId, eduPersonOrcid の設定例を追加しました。
デフォルトの名前空間の宣言が3系になって抜けていたので足しました。<resolver:AttributeDefinition>のような書き方に加えて名前空間を省略した形（<AttributeDefinition>等）でも記述できます。
従来コメントアウトされていた LDAP Connector を有効化しました。

Shibboleth IdP 3.2.0向けテンプレート

※[upki-fed:01034]のReturnAttributesの件ですが、本テンプレートではデフォルトで記述されておりません。つまりldap.propertiesの記述によらず全てのLDAP属性を取得します。ldap.propertiesの`idp.attribute.resolver.LDAP.returnAttributes`の設定を反映したい場合はテンプレート内のコメントに従って修正してください。
gakuninScopedPersonalUniqueCode の設定例で誤って Simple Attribute Definition を使っていたところを Prescoped Attribute Definition に修正しました。

ダウンロード: attribute-resolver-template-2.0.1.xml
学認技術運用基準(v2.0)に新たに追加された属性 gakuninScopedPersonalUniqueCode, isMemberOf の設定例を追加しました。

ダウンロード: attribute-resolver-template-2.0.0.xml, attribute-filter-template-prodfed-2.0.0.xml, attribute-filter-template-testfed-2.0.0.xml
各属性に割り当てるid(attributeID)をシステム運用基準に合わせる形で以下のように修正しました。今後SP接続情報等で掲載する情報はこちらを元にしたものになります。また、更新する場合は**attribute-resolver.xml/attribute-filter.xml両方を同時に**行わないと不整合が生じます。みなさまにおかれましてはIdPの属性設定ファイルの最新版（バージョン1.2.x）への更新をご検討ください。

- email → mail
- organizationalUnit → organizationalUnitName
- jaorganizationName → jaOrganizationName
- jaorganizationalUnit → jaOrganizationalUnitName
- jadisplayName → jaDisplayName
- jagivenName → jaGivenName
- jasurname → jaSurname

~~※ jaSurnameおよびsurnameは現行の学認技術運用基準(v2.0)での表記と異なりますが、技術運用基準を修正予定です。~~→v2.1で修正されました。(2015-03-12)

ダウンロード: attribute-resolver-template-1.2.0.xml, attribute-filter-template-prodfed-1.2.0.xml, attribute-filter-template-testfed-1.2.0.xml
ダウンロード: attribute-resolver-template-1.0.1.xml, attribute-filter-template-prodfed-1.0.1.xml, attribute-filter-template-testfed-1.0.1.xml

- 属性設定テンプレート（SP用）
  - attribute-map.xml
    このファイルについて詳しくは、SPカスタマイズの属性の追加方法をご覧ください。
    ⇒属性の追加方法
  - attribute-policy.xml
    gakuninScopedPersonalUniqueCodeのScopingRulesを追加しています。その他、IdPから渡された属性をフィルタしてアプリケーションに渡す場合には適宜設定を追加してください。

更新情報2023年8月24日(3.4.0)

Shibboleth SP 3.4.x 向けテンプレート - 3.4.1 の配布物をベースとして再作成しました。（フラット化されております）

更新情報2019年7月18日(3.3.0)

Shibboleth SP 3.0.x向けテンプレート - 3.0の配布物をベースとして再作成しました。
特にattribute-map-template.xmlについては、targeted-idの削除、unscoped-affiliationのコメントアウト、eppnへのcaseSensitive="false" の指定の追加などが行われております。
unscoped-affiliation(eduPersonAffiliation)のコメントアウトはShibboleth開発元の使うべきでないという意向に合わせたものです。引き続きこれを使う必要がある場合は有効化してお使いください。関連課題

更新情報2018年8月23日(3.2.2)

学認技術運用基準(v2.2)に新たに追加された属性 eduPersonAssurance, eduPersonUniqueId, eduPersonOrcid を追加しました。

一部のja属性に欠けていたcaseSensitive設定を付与しました。Apacheのrequire構文等で大文字小文字が区別されなくなります。

Shibboleth SP 2.6.0の配布物をベースとして再作成しました。
学認技術運用基準(v2.0)に新たに追加された属性 gakuninScopedPersonalUniqueCode, isMemberOf を追加しました。attribute-policy-template.xmlは gakuninScopedPersonalUniqueCode のスコープチェックのため今回新たに作成されました。

- メタデータテンプレート
  - IdPメタデータテンプレート
  - SPメタデータテンプレート

配布している属性設定テンプレートのファイル名と最新バージョンの対応は以下の通りです。Shibboleth IdP/SPのバージョンとは対応しておりませんのでご注意ください。

ファイル名	最新バージョン	ベースとなるShibboleth IdP/SPバージョン

attribute-resolver-template.xml	4.2.0	4.2.1
attribute-filter-template-prodfed.xml	4.0.0	4.0.1
attribute-filter-template-testfed.xml	4.0.0	4.0.1
gakunin-rules.tar.gz	4.0.0	4.0.1
attribute-map-template.xml	3.3.0	3.0.4
attribute-policy-template.xml	3.4.0	3.4.1

開発ツール

学術認証フェデレーションで開発したツールを提供公開しています。

- ユーザ同意取得システム：uApproveJP (uApprove Jet Pack)

以下のツールはShibboleth IdPバージョン2向けです。

- 旧: FPSP（Filter Per SP, ユーザに対する特定SPへのアクセス制限）プラグイン
- 旧: IdPにおけるSP利用同意プラグイン (SPToUプラグイン)